

RECORDER

Publication number: JP2001309159

Publication date: 2001-11-02

Inventor: MORIFUJI HAJIME; IWAMI NAOKO; YOSHIURA YUTAKA; KONNO CHISATO; KUROSU YUTAKA

Applicant: HITACHI LTD

Classification:

- international: **B41J29/00; B41J5/30; G06T1/00; H04N1/387; H04N5/225; H04N101/00; B41J29/00; B41J5/30; G06T1/00; H04N1/387; H04N5/225; (IPC1-7): H04N1/387; B41J5/30; B41J29/00; G06T1/00; H04N5/225; H04N101/00**

- European:

Application number: JP20000126235 20000420

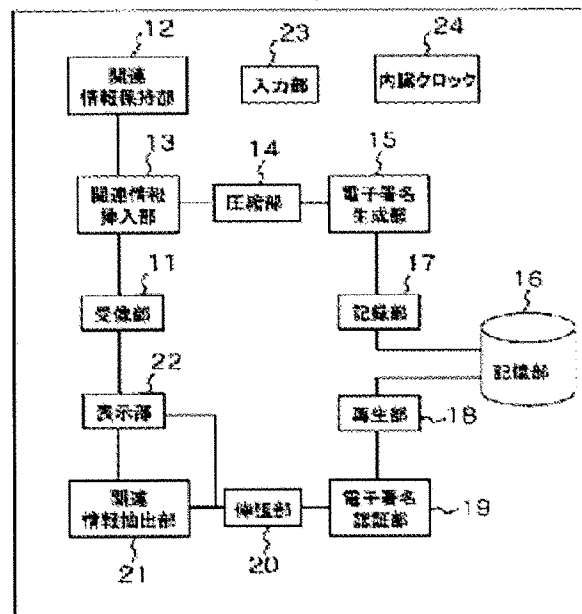
Priority number(s): JP20000126235 20000420

Report a data error here

Abstract of JP2001309159

PROBLEM TO BE SOLVED: To provide a recorder that can suitably prevent falsification of generated digital image data and enhance the reliability as evidence. **SOLUTION:** A relating information insertion section 13 utilizes an electronic watermark technology to imbed relating information of digital image data stored in a relating information storage section 12 to the digital image data obtained by an image receiver section 11. An electronic signature generating section 15 generates an electronic signature of the digital image data to which the relating information is imbedded. A recording section 17 adds the electronic signature to the digital image data to which the relating information is imbedded and stores the resulting data to a storage section 16.

図1



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-309159

(P2001-309159A)

(43) 公開日 平成13年11月2日 (2001.11.2)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 N 1/387		H 0 4 N 1/387	2 C 0 6 1
B 4 1 J 5/30		B 4 1 J 5/30	Z 2 C 0 8 7
	29/00	G 0 6 T 1/00	5 0 0 B 5 B 0 5 7
G 0 6 T 1/00	5 0 0	H 0 4 N 5/225	F 5 C 0 2 2
H 0 4 N 5/225		101: 00	5 C 0 7 6

審査請求 未請求 請求項の数12 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願2000-126235(P2000-126235)

(22) 出願日 平成12年4月20日 (2000.4.20)

特許法第30条第1項適用申請有り 平成11年10月21日～
10月22日 情報処理学会コンピュータセキュリティ研究
会主催の「コンピュータセキュリティシンポジウム'
99」において文書をもって発表

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 森藤 元

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72) 発明者 岩見 直子

東京都千代田区神田駿河台四丁目6番地
株式会社日立製作所研究開発本部内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

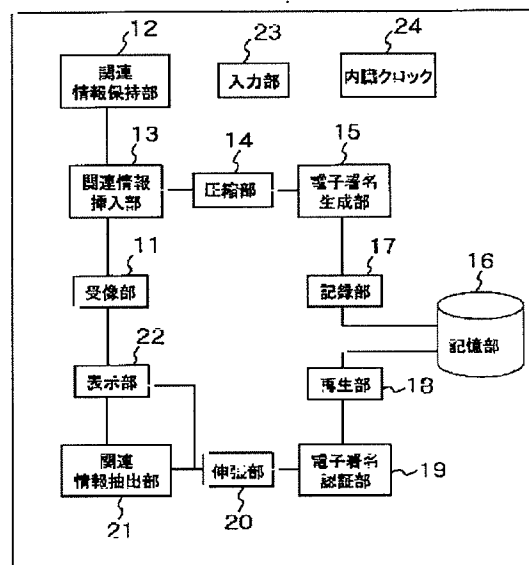
(54) 【発明の名称】 記録装置

(57) 【要約】

【課題】生成したデジタル画像データの改竄防止や証拠
としての信頼性向上に好適な記録装置を提供する。

【解決手段】関連情報挿入部13は、電子透かし技術を利用
して、受像部11で得たデジタル画像データに、関連
情報保持部12で保持した当該デジタル画像データの
関連情報を埋め込む。電子署名生成部15は、この関連
情報が埋め込まれたデジタル画像データの電子署名を
作成する。記録部17は、関連情報が埋め込まれたデジ
タル画像データに前記電子署名を付加して、記憶部16に
記憶する。

図1



【特許請求の範囲】

【請求項1】映像を撮像してデジタル画像データに変換して記録する記録装置であって、前記デジタル画像データの電子署名を作成する電子署名手段と、前記デジタル画像データに前記電子署名を付加して記憶媒体に記憶する記憶手段と、を備えることを特徴とする記録装置。

【請求項2】請求項1記載の記録装置であって、前記デジタル画像データに付加された電子署名を用いて、当該デジタル画像データを認証する認証手段をさらに備えることを特徴とする記録装置。

【請求項3】映像を撮像してデジタル画像データに変換する記録装置であって、電子透かし技術を利用して、前記デジタル画像データに当該デジタル画像データの関連情報を埋め込む電子透かし手段と、前記関連情報が埋め込まれたデジタル画像データを記憶媒体に記憶する記憶手段と、を備えることを特徴とする記録装置。

【請求項4】請求項3記載の記録装置であって、前記電子透かし手段は、前記デジタル画像データを複数の領域に分割し、当該分割された複数の領域の少なくとも1つに対して、前記デジタル画像データの関連情報を埋め込み、且つ、当該関連情報が埋め込まれた領域を含む前記分割された複数の領域を統合して、前記関連情報が埋め込まれたデジタル画像データを生成することを特徴とする記録装置。

【請求項5】請求項3記載の記録装置であって、前記電子透かし手段は、前記デジタル画像データを複数の領域に分割するとともに、当該デジタル画像データの関連情報を複数の領域に分割して各々を前記複数の領域各々に対応させ、前記複数の領域各々に対して、複数の分割された前記関連情報の対応する部分を埋め込み、且つ、各々に前記関連情報の対応する部分が埋め込まれた前記複数の領域を統合して、前記関連情報が埋め込まれたデジタル画像データを生成することを特徴とする記録装置。

【請求項6】請求項3、4または5記載の記録装置であって、電子透かし技術を利用して、前記デジタル画像データに埋め込まれた関連情報を抽出する関連情報抽出手段をさらに備えることを特徴とする記録装置。

【請求項7】映像を撮像してデジタル画像データに変換する記録装置であって、電子透かし技術を利用して、前記デジタル画像データに当該デジタル画像データの関連情報を埋め込む電子透かし手段と、前記関連情報が埋め込まれたデジタル画像データの電子署名を作成する電子署名手段と、前記関連情報が埋め込まれたデジタル画像データに前記

電子署名を付加して記憶媒体に記憶する記憶手段と、を備えることを特徴とする記録装置。

【請求項8】請求項7記載の記録装置であって、前記関連情報が埋め込まれたデジタル画像データに付加された電子署名を用いて、当該関連情報が埋め込まれたデジタル画像データを認証する認証手段と、電子透かし技術を利用して、前記デジタル画像データに埋め込まれた関連情報を抽出する関連情報抽出手段と、をさらに備えることを特徴とする記録装置。

【請求項9】請求項7記載の記録装置であって、前記関連情報が埋め込まれたデジタル画像データを圧縮する圧縮手段をさらに備え、前記電子署名手段は、前記圧縮されたデータの電子署名を作成し、前記記憶手段は、前記圧縮されたデータに前記電子署名を付加して記憶媒体に記憶することを特徴とする記録装置。

【請求項10】請求項9記載の記録装置であって、前記圧縮されたデータに付加された電子署名を用いて、当該圧縮されたデータを認証する認証手段と、前記圧縮されたデータを伸張して、前記関連情報が埋め込まれたデジタル画像データを生成する伸張手段と、電子透かし技術を利用して、前記伸張されたデジタル画像データに埋め込まれた関連情報を抽出する関連情報抽出手段と、をさらに備えることを特徴とする記録装置。

【請求項11】請求項7記載の記録装置であって、前記デジタル画像データを圧縮する圧縮手段をさらに備え、前記電子透かし手段は、電子透かし技術を利用して、前記圧縮されたデータに前記デジタル画像データの関連情報を埋め込み、前記電子署名手段は、前記関連情報が埋め込まれた、圧縮されたデータの電子署名を作成し、前記記憶手段は、前記関連情報が埋め込まれた、圧縮されたデータに前記電子署名を付加して記憶媒体に記憶することを特徴とする記録装置。

【請求項12】請求項11記載の記録装置であって、前記関連情報が埋め込まれた、圧縮されたデータに付加された電子署名を用いて、当該関連情報が埋め込まれた、圧縮されたデータを認証する認証手段と、電子透かし技術を利用して、前記圧縮されたデータに埋め込まれた関連情報を抽出する関連情報抽出手段と、前記関連情報が埋め込まれた、圧縮されたデータを伸張して、前記デジタル画像データを生成する伸張手段と、をさらに備えることを特徴とする記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、映像を撮像してデジタル画像データに変換する記録装置に関し、特に、生成したデジタル画像データの改竄防止や証拠としての信

頼性向上に好適な技術に関する。

【0002】

【従来の技術】従来より、レンズで捉えた光学像をCCD (Charge Coupled Device) 等の撮像素子で電気信号に変換し、得られた画像データをデジタル形式で記録する電子カメラなどの記録装置が知られている。近年では、撮像素子などの性能向上に伴い、銀塩写真並の画質を得ることも可能となりつつあり、このため、各種証明や証拠撮影に、通常のカメラに代えて電子カメラが採用されることも考えられ得る。

【0003】

【発明が解決しようとする課題】ところで、デジタル画像データは、コンピュータにより容易に編集・複製することができるという特質を有する。このため、電子カメラなどの記録装置を各種証明や証拠などの撮影に使用した場合、通常のカメラの場合に比べて、より巧妙に不正が行われる可能性がある。

【0004】たとえば、電子カメラで得た他人のデジタル画像データを勝手に複製して各種証明や証拠に使用したり、あるいは、電子カメラで得たデジタル画像データを編集して、撮影時の映像に変更を加え、これを各種証明や証拠などに使用することが考えられ得る。このような場合、通常のカメラで得た銀塩写真の場合に比べて不正の検出が容易でない。

【0005】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、生成したデジタル画像データの改竄防止や証拠としての信頼性向上に好適な電子カメラなどの記録装置を提供することにある。

【0006】

【課題を解決するための手段】上記課題を解決するために、本発明の第1の態様は、映像を撮像してデジタル画像データに変換する電子カメラなどの記録装置であって、前記デジタル画像データの電子署名を作成する電子署名手段と、前記デジタル画像データに前記電子署名を付加して記憶媒体に記憶する記憶手段と、を備えることを特徴とする。

【0007】ここで、前記デジタル画像データに付加された電子署名を用いて、当該デジタル画像データを認証する認証手段をさらに備えるようにしてもよい。

【0008】なお、本態様の電子署名手段および認証手段に利用する電子署名技術としては、たとえば、「A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms」(IEEE Trans. On Inform. Theory, Vol. IT31, No. 4, pp. 469-472, 1985)に記載の技術が挙げられる。具体的には、電子署名手段において、デジタル画像データを1方向関数であるハッシュ関数で評価し、評価結果であるハッシュ値を公開鍵暗号体系にしたがった秘密鍵(署名鍵)で暗号化することで、当該デジタル画像データの電子署名を作成する。一方、認証手段では、前記デジタル画像データに付加された電

子署名を前記秘密鍵と対の公開鍵(検証鍵)で復号化してハッシュ値を得、これを、前記デジタル画像データを前記ハッシュ関数で評価することで得たハッシュ値と比較する。そして、両者が一致する場合は、前記デジタル画像データは、当該デジタル画像データの電子署名の作成後、変更されていないものとして認証する。

【0009】本態様によれば、映像を撮像することで得られたデジタル画像データに、当該データの電子署名が付加されて記憶媒体に記憶されるので、当該電子署名を用いて認証を行うことにより、電子署名作成後に当該データに加えられた変更を検出することができる。電子署名は映像撮影時に電子カメラなどの記録装置内で作成されるので、各種証明や証拠などの撮影に使用した場合、デジタル画像データの改竄などの不正を容易に検出することができる。

【0010】本発明の第2の態様は、映像を撮像してデジタル画像データに変換する記録装置であって、電子透かし技術を利用して、前記デジタル画像データに当該デジタル画像データの関連情報を埋め込む電子透かし手段と、前記関連情報が埋め込まれたデジタル画像データを記憶媒体に記憶する記憶手段と、を備えることを特徴とする。

【0011】ここで、電子透かし技術を利用して、前記デジタル画像データに埋め込まれた関連情報を抽出する関連情報抽出手段をさらに備えるようにしてもよい。

【0012】なお、電子透かし技術とは、所定の情報を、デジタル画像データに、所定の規則にしたがい、たとえば前記デジタル画像データの輝度情報に変更を加えることで、少なくとも前記所定の規則を用いることなく当該所定の情報を当該デジタル画像データから抽出できないように埋め込む技術である。前記所定の情報を前記デジタル画像データから抽出する際に、原デジタル画像データ(前記所定の情報を埋め込む前のデジタル画像データ)を参照するものと、参照しないものがある。本態様の関連情報抽出手段には、原デジタル画像データを参照することなく、関連情報をデジタル画像データから抽出することができる技術を利用することが好ましい。このような技術としては、たとえば「ピクセルブロックによる静止画像データハイディング」(In Proc. of IPSJ 56th annual conference, 1998)に記載の技術が挙げられる。

【0013】本態様によれば、映像を撮像することで得られたデジタル画像データに、当該データの関連情報、たとえば撮影日時や撮影者や撮影場所などの著作権情報が埋め込まれて記憶媒体に記憶されるので、当該デジタル画像データから関連情報を抽出し、その内容を確認することができる。関連情報の埋め込みは、映像撮影時に記録装置内で行われるので、各種証明や証拠などの撮影に使用した場合、デジタル画像データの証拠としての信頼性を向上させることができる。

【0014】なお、本態様において、前記電子透かし手段は、前記デジタル画像データを複数の領域に分割し、当該分割された複数の領域の少なくとも1つに対して、前記デジタル画像データの関連情報を埋め込み、且つ、当該関連情報が埋め込まれた領域を含む前記分割された複数の領域を統合して、前記関連情報が埋め込まれたデジタル画像データを生成するものであってもよい。

【0015】このようにすることで、関連情報の埋め込みは、複数の領域に分割されたデジタル画像データの任意の領域に対して行われるので、デジタル画像データ全体に対して関連情報を埋め込む場合に比べ、関連情報の埋め込みに使用するメモリのワークエリアやCPUの負荷を小さくすることができる。このことは、小型・軽量化が望まれる記録装置に特に有効である。

【0016】なお、複数の領域に分割されたデジタル画像データの任意の領域に対して関連情報の全てを埋め込んだ場合、当該領域の画質の劣化が危惧される場合は、前記電子透かし手段を以下のように修正してもよい。すなわち、関連情報を複数の領域に分割して各々を前記複数の領域各々に対応させる。そして、前記複数の領域各々について、当該領域に、複数の領域に分割された前記関連情報の対応する部分を埋め込む処理を順次行い、その後、各々に前記関連情報の対応する部分が埋め込まれた前記複数の領域を統合して、前記関連情報が埋め込まれたデジタル画像データを生成する。

【0017】本発明の第3の態様は、映像を撮像してデジタル画像データに変換する記録装置であって、電子透かし技術を利用して、前記デジタル画像データに当該デジタル画像データの関連情報を埋め込む電子透かし手段と、前記関連情報が埋め込まれたデジタル画像データの電子署名を作成する電子署名手段と、前記関連情報が埋め込まれたデジタル画像データに前記電子署名を付加して記憶媒体に記憶する記憶手段と、を備えることを特徴とする。

【0018】ここで、前記関連情報が埋め込まれたデジタル画像データに付加された電子署名を用いて、当該関連情報が埋め込まれたデジタル画像データを認証する認証手段と、電子透かし技術を利用して、前記デジタル画像データに埋め込まれた関連情報を抽出する関連情報抽出手段と、をさらに備えるようにしてもよい。

【0019】本態様によれば、映像を撮像することで得られたデジタル画像データに、当該データの関連情報が埋め込まれ、さらに、当該関連情報が埋め込まれたデジタル画像データに、当該データの電子署名が付加されて記憶媒体に記憶されるので、当該電子署名を用いて認証を行うことにより、電子署名作成後に当該データに加えられた変更を検出することができ、また、当該データから関連情報を抽出し、その内容を確認することができる。したがって、各種証明や証拠などの撮影に使用した場合、デジタル画像データの改竄などの不正を検出する

ことができるとともに証拠としての信頼性を向上させることができる。

【0020】なお、本態様において、前記関連情報が埋め込まれたデジタル画像データを圧縮する圧縮手段をさらに備え、前記電子署名手段は、前記圧縮されたデータの電子署名を作成し、前記記憶手段は、前記圧縮されたデータに前記電子署名を付加して記憶媒体に記憶するものであってもよい。

【0021】あるいは、前記デジタル画像データを圧縮する圧縮手段をさらに備え、前記電子透かし手段は、電子透かし技術を利用して、前記圧縮されたデータに前記デジタル画像データの関連情報を埋め込み、前記電子署名手段は、前記関連情報が埋め込まれた、圧縮されたデータの電子署名を作成し、前記記憶手段は、前記関連情報が埋め込まれた、圧縮されたデータに前記電子署名を付加して記憶媒体に記憶するものであってもよい。

【0022】このようにすることで、両者とも、記憶媒体に記憶する情報量を減らすことができる。ただし、前者では、デジタル画像データに当該関連情報が埋め込まれた後に、当該データが圧縮されるのに対し、後者では、デジタル画像データが圧縮された後に当該関連情報が埋め込まれるため、前者の方が、当該関連情報が原デジタル画像データに与える影響をより低減させることができる。

【0023】

【発明の実施の形態】以下に、本発明の第1実施形態について説明する。

【0024】図1は、本発明の第1実施形態が適用された電子カメラの機能構成図である。

【0025】ここで、受像部11は、レンズで捉えた光学像をCCD (Charge Coupled Device) やMOS (Metal-Oxide Semiconductor) 等の撮像素子で電気信号に変換し、これをデジタル画像データに変換する。

【0026】関連情報保持部12は、受像部11で得たデジタル画像データの関連情報、たとえば、撮影日時や撮影者や撮影場所や撮影に使用した記録装置を特定することができる情報（装置の製造番号等）などの情報（著作権情報）を保持する。ここで、撮影者の情報や撮影に使用した記録装置を特定することができる情報（装置の製造番号等）は、たとえば、入力部23を介して操作者より受け付けたものを予め登録しておくようにしてもよい。また、撮影日時に関する情報は、内蔵クロック24より取得するようにしてもよい。また、撮影場所に関する情報は、入力部23を介して、撮影の都度、操作者より受け付けるようにしてもよいし、あるいは、GPS技術を利用して現在地を算出する現在地算出部を設け、撮影時に、当該算出部が算出した現在位置を撮影場所とするようにしてもよい。

【0027】関連情報挿入部13は、電子透かし技術を利用して、受像部11で得たデジタル画像データに、関連情報保持部12が保持する当該デジタル画像データの

関連情報を埋め込む。なお、電子透かし技術とは、上述したように、所定の情報を、デジタル画像データに、所定の規則にしたがい、たとえば前記デジタル画像データの輝度情報に変更を加えることで、少なくとも前記所定の規則を用いることなく当該所定の情報を当該デジタル画像データから抽出できないように埋め込む技術である。前記所定の情報を前記デジタル画像データから抽出するに際し、原デジタル画像データ（前記所定の情報を埋め込む前のデジタル画像データ）を参照するものと、参照しないものがある。本実施形態では、後者の技術を利用することとする。このような技術としては、たとえば「ピクセルブロックによる静止画像データハイディング」(In Proc. of IPSJ 56th annual conference, 1998)に記載の技術が挙げられる。

【0028】圧縮部14は、たとえば「ISO International Standard 10918 Part1」で定義されているJPEG (Joint Photographic Coding Experts Group) 方式にしたがって、関連情報挿入部13により関連情報が埋め込まれたデジタル画像データを圧縮する。

【0029】電子署名生成部15は、圧縮部14で圧縮された、関連情報が埋め込まれたデジタル画像データ等に対して、電子署名を生成する。なお、電子署名技術としては、たとえば、「A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms」(IEEE Trans. On Inform. Theory, Vol.IT31, No.4, p.469-472, 1985)に記載の技術が挙げられる。具体的には、圧縮部14で圧縮されたデータ等を1方向関数であるハッシュ関数で評価し、評価結果であるハッシュ値を公開鍵暗号体系にしたがった秘密鍵（署名鍵）で暗号化することで電子署名を作成する。

【0030】記憶部16は、可搬性を有するフラッシュメモリなどの記憶媒体が挿抜可能に構成されている。

【0031】記録部17は、記憶部16に装着された記憶媒体に、圧縮部14で圧縮された、関連情報が埋め込まれたデジタル画像データを、電子署名生成部15で生成した電子署名を付加して記録させる。図2は、圧縮部14での圧縮にJPEG方式を用いた場合において、記憶部16に装着された記憶媒体に記録されるデータの構成を示した図である。図示するように、JPEG方式による圧縮データファイルは、圧縮された画像データが格納される圧縮画像データ格納エリア220と、圧縮データファイル全体の大きさや圧縮画像データ格納エリア220の大きさやエラー訂正情報等の圧縮画像データ格納エリア220に格納されている圧縮画像データの構成に関する情報などが格納される構成情報格納エリア230とからなる。そして、構成情報格納エリア230には、ユーザが定義可能な拡張エリアであるユーザ定義エリア (Application Data Segment) 240が設けられている。

【0032】記録部17は、たとえば、電子署名生成部

15で生成した電子署名をこのユーザ定義エリア240に格納することで、圧縮部14で圧縮されたデータに電子署名を付加して記録させる。

【0033】電子署名の署名対象データとしては、圧縮画像データ格納エリア220に格納されているデータだけでなく、構成情報格納エリア230に格納されているデータも含めてよい。この場合、署名生成時にユーザ定義エリア240内の電子署名を格納する領域は署名の対象から除外する。あるいは、該領域に署名検証時に同一に復元可能な情報をダミーデータ（たとえば0）として挿入した上で電子署名を生成してもよい。

【0034】再生部18は、記憶部16に装着されている記憶媒体に記録された圧縮画像データと当該データに付加された電子署名を読み出す。

【0035】電子署名認証部19は、再生部18が読み出した電子署名を用いて、当該電子署名が付加された圧縮画像データの認証を行う。この電子署名認証部19は、電子署名生成部15と対になるものであり、具体的には、電子署名生成部15にてハッシュ値を暗号化するのに用いた秘密鍵と対の公開鍵（検証鍵）を用いて電子署名を復号化し、ハッシュ値を復元する。また、当該電子署名が付加された電子署名対象データを、電子署名生成部15にてハッシュ値を生成するのに用いたハッシュ関数で評価し、評価結果であるハッシュ値を生成する。そして、復元したハッシュ値と生成したハッシュ値とを比較し、両者が一致する場合は、電子署名対象データが当該データの電子署名の作成後、変更されていないものとして認証する。

【0036】伸張部20は、圧縮部14と対になるものであり、電子署名認証部19で認証された圧縮画像データを、圧縮部14での圧縮方式に応じた伸張方式にしたがって伸張し、関連情報が埋め込まれたデジタル画像データを復元する。

【0037】関連情報抽出部21は、伸張部20で伸張された、関連情報が埋め込まれたデジタル画像データより、当該関連情報を抽出する。この関連情報抽出部21は、関連情報挿入部13と対になるものであり、関連情報挿入部13において、デジタル画像データに関連情報を埋め込む際に用いた所定の規則にしたがい、当該デジタル画像データから関連情報を抽出する。上述したように、本実施形態では、原デジタル画像データ（関連情報を埋め込む前のデジタル画像データ）を参照することなく、関連情報をデジタル画像データから抽出する技術を利用する。

【0038】表示部11は、たとえば液晶パネルなどで構成されており、受像部11で得たデジタル画像データや伸張部20で伸張したデジタル画像データ、あるいは、関連情報抽出部21で抽出した関連情報などを表示する。

【0039】次に、本実施形態が適用された電子カメラ

のハードウェア構成について説明する。

【0040】図3は、図1に示す電子カメラのハードウェア構成の一例を示す図である。

【0041】ここで、CCD51、バッファ52、A/D変換器53、タイミング発生器(TG)54、および、駆動回路55は、図1に示す受像部11を構成する。すなわち、レンズで捉えた光学像がCCD51で電気信号に変換され、バッファ52を介して増幅等の処理が行われた後、A/D変換器53によりデジタル画像データに変換され、タイミング発生器54に入力される。タイミング発生器54は、タイミング信号を発生してCCD51を駆動する駆動回路55を制御するとともに、このタイミング信号にしたがってデジタル画像データをデータバス80へ送出する。

【0042】フラッシュメモリ58は、コネクタ59に挿抜自在に構成されている。フラッシュメモリ58およびコネクタ59は、図1に示す記憶部16を構成する。

【0043】DRAM(Dynamic RAM)56は、タイミング発生器54からデータバス80上へ送出されたデジタル画像データや、コネクタ59を介してフラッシュメモリ58からデータバス80上へ送出されたデータ、あるいは、圧縮・伸張回路57よりデータバス80上へ送出されたデータなどを一時的に保持する。なお、デジタル画像データは、CPU63による演算により輝度信号と色差信号に分離されてDRAM56に格納される。

【0044】圧縮・伸張回路57は、図1に示す圧縮部14および伸張部20を構成する。

【0045】すなわち、JPEG方式にしたがって、DRAM56に格納されたデジタル画像データを圧縮したり、圧縮されたデジタル画像データを伸張したりする。

【0046】ビデオ信号発生器(SG)60、D/A変換器61、および、液晶ディスプレイ(LCD)62は、図1に示す表示部22を構成する。すなわち、データバス上のデジタル画像データは、CPU63の指示にしたがい、ビデオ信号発生器60に取り込まれ、そこで同期信号等が付加されてデジタルビデオ信号に変換される。このデジタルビデオ信号は、D/A変換器61でアナログ信号に変換され、液晶ディスプレイ62へ出力される。

【0047】キー入力装置66は、図1に示す入力部23として機能するものであり、電子カメラの動作モード(撮影、再生等)や各種設定値を受け付けるためのスイッチや、記録の指示を受け付けるためのシャッターボタン等より構成される。

【0048】クロック67は、図1に示す内蔵クロック24として機能するものであり、時刻情報を生成する。I/Oポート68は、シリアル信号に変換された映像信号等を入出力するインターフェースとして機能する。

【0049】ROM64には、電子カメラを構成する各部を統括的に制御するためのプログラムや、関連情報の

デジタル画像データへの埋め込みや抽出(電子透かし技術)のためのプログラムや、電子署名の作成や認証(電子署名技術)のためのプログラムなどが格納されている。また、電子署名の作成や認証に用いる公開鍵暗号体系にしたがった秘密鍵と公開鍵が格納されている。なお、ROM64は、電子カメラに固定的に与えられるものでもよいし、あるいは、メモリカードなどの挿抜可能な形態で電子カメラに与えられるものでもよい。

【0050】CPU63は、ROM64に格納された各種プログラムを実行することで、電子カメラを構成する各部を統括的に制御する。また、図1に示す関連情報挿入部13、関連情報抽出部21、電子署名生成部15、電子署名認証部19、記録部17、および、再生部18を、プロセスとして実現する。

【0051】RAM65は、CPU63のワークエリアとして機能する。また、図1に示す関連情報保持部12を構成する。

【0052】次に、本実施形態が適用された電子カメラの動作について説明する。

【0053】まず、本実施形態が適用された電子カメラの撮影時の動作を説明する。

【0054】図4は、図1に示す電子カメラの撮影時の動作を説明するためのフロー図である。

【0055】このフローは、入力部23で受け付けた操作者の指示より、動作モードとして、撮影モードが選択されている場合に実行される。

【0056】まず、受像部11は、レンズで捉えた光学像を電気信号に変換し、さらにデジタル画像データに変換して表示部22に送る(ステップS101)。表示部22は、受け取ったデジタル画像データにしたがった画像を表示する(ステップS102)。

【0057】次に、受像部11は、入力部23を介して、デジタル画像データの記録指示が入力されたか否か、すなわち、シャッターボタンが押されたか否かを判断し(ステップS103)、押された場合にはステップS104へ移行し、押されていない場合はステップS101に戻る。

【0058】ステップS104では、関連情報挿入部13は、入力部23を介して操作者より選択された撮影モードが、デジタル画像データに関連情報を埋め込んで電子署名を採る証拠写真モードであるか否かを判断する。この判断は、入力部23を介して操作者より撮影モードが選択された際に、たとえば図5(a)に示すような、それが証拠写真モードであるか通常の写真モードであるかを示すフラグを、図3に示すRAM65の所定領域に記憶させておくことで実現できる。

【0059】ステップS104において、証拠写真モードであると判断した場合は、受像部11からデジタル画像データを取得し、これに、電子透かし技術を利用して、関連情報保持部12に保持されている関連情報を埋

め込む(ステップS105)。

【0060】そして、この関連情報が埋め込まれたデジタル画像データを圧縮部14へ渡す。

【0061】一方、証拠写真モードでないと判断した場合は、受像部11から取得したデジタル画像データを、関連情報を埋め込むことなく圧縮部14へ渡す。

【0062】次に、圧縮部14は、関連情報挿入部13から受け取ったデジタル画像データあるいは関連情報が埋め込まれたデジタル画像データを、所定の圧縮方式にしたがって圧縮し(ステップS106)、圧縮結果である圧縮画像データを電子署名生成部15に渡す。

【0063】次に、電子署名生成部15は、入力部23を介して操作者より選択された撮影モードが証拠写真モードであるか否かを判断する(ステップS107)。証拠写真モードであると判断した場合は、圧縮部14より受け取った圧縮画像データの電子署名を生成し(ステップS108)、生成した電子署名を圧縮画像データとともに記録部17へ渡す。一方、証拠写真モードでないと判断した場合は、圧縮部14より受け取った圧縮画像データを、電子署名を生成することなく記録部17へ渡す。

【0064】次に、記録部109は、電子署名生成部15より受け取った圧縮画像データを記憶部16に装着されている記憶媒体に記憶する(ステップS109)。この際、電子署名生成部15より、圧縮画像データとともに当該データの電子署名を受け取っている場合は、当該データにこの電子署名を付加して記憶する。

【0065】このようにすることで、撮影モードとして証拠写真モードが選択されている場合、撮影により得たデジタル画像データに当該データの関連情報が埋め込まれた後、圧縮され、この圧縮画像データの電子署名が作成される。そして、圧縮画像データが電子署名とともに記憶媒体に記録される。

【0066】次に、本実施形態が適用された電子カメラの画像再生時の動作を説明する。

【0067】図6は、図1に示す電子カメラの画像再生時における動作を説明するためのフロー図である。

【0068】このフローは、入力部23で受け付けた操作者の指示より、動作モードとして、再生モードが選択されている場合に実行される。

【0069】まず、再生部18は、記録部16に装着されている記憶媒体より、圧縮画像データ(図4に示すフローにより記憶媒体に記録されたデータ)を読み出し(ステップS201)、電子署名認証部19に渡す。なお、圧縮画像データに電子署名が付加されている場合は、これも読み出して電子署名認証部19に渡す。

【0070】次に、電子署名認証部19は、再生部18から受け取った圧縮画像データに電子署名が付加されているか否かを調べることで、当該圧縮画像データが証拠写真モードで撮影されたものであるか否かを判断する

(ステップS202)。証拠写真モードで撮影されたものである場合、たとえば図5(b)に示すような、証拠写真モードである旨を示すフラグ「1」を図3に示すRAM65等の所定領域に記憶させ、ステップS203に移行する。一方、証拠写真モードで撮影されたものでない場合は、たとえば図5(b)に示すような、通常の写真モードである旨を示すフラグ「0」を図3に示すRAM65等の所定領域に記憶させ、ステップS204に移行する。

【0071】ステップS203では、電子署名認証部19は、圧縮画像データに付加された電子署名を用いて、当該圧縮画像データの認証を行う。

【0072】電子署名の署名対象データとして、構成情報格納エリア230に格納されているデータも含めていた場合は、電子署名生成時の処理に対応させて、ユーザ定義エリア240内の電子署名を格納する領域を署名の対象から除外するか、あるいは、該領域に署名生成時に挿入したものと同一の情報(ダミーデータ)と置換した上で電子署名を検証する。

【0073】なお、電子署名の対象データに何が含まれるか、電子署名はどこに格納されているか、署名生成時にどのような処理が行われたか、などの情報は、あらかじめ電子カメラを使用するシステムに共通の情報として知られているものとする。

【0074】そして、認証の結果を記憶する。たとえば図5(c)に示すような、圧縮画像データが改竄されたか否かを示すフラグを、図3に示すRAM65の所定領域に記憶させる。

【0075】ステップS204では、伸張部20は、電子署名認証部19より圧縮画像データを受け取り、これを伸張して、デジタル画像データを得る。

【0076】次に、関連情報抽出部21は、ステップS202で立てたフラグを調べ、伸張部20で伸張されたデジタル画像データが証拠写真モードで撮影されたものであるか否かを判断する(ステップS205)。証拠写真モードで撮影されたものである場合は、図4に示すフローにより、当該デジタル画像データに、その関連情報が埋め込まれているので、ステップS206に移行し、電子透かし技術を利用して、当該デジタル画像データから関連情報を抽出する。それから、当該デジタル画像データを表示部22に渡し、表示画面に表示させる(ステップS207)。一方、証拠写真モードで撮影されたものでない場合は、当該デジタル画像データを直ちに表示部22に渡し、表示画面に表示させる(ステップS207)。

【0077】次に、表示部22は、ステップS202で立てたフラグを調べ、表示中のデジタル画像データが証拠写真モードで撮影されたものであるか否かを判断する(ステップS208)。証拠写真モードで撮影されたものでない場合は、ステップS209に移行し、入力部2

3を介して、操作者より画像の送り・戻し指示が入力されたか否かを判断する。画像の送り・戻し指示が入力された場合、当該指示により特定される圧縮画像データを記憶部16の記憶媒体から読み出すべく、ステップS201に戻る。一方、画像の送り・戻し指示が入力されていない場合はステップS207に戻る。

【0078】ステップS208において、表示中のデジタル画像データが証拠写真モードで撮影されたものと判断された場合、ステップS210に移行し、入力部23を介して、操作者より関連情報の表示指示が入力されたか否かを判断する。関連情報の表示指示が入力されていない場合はステップS209に移行する。一方、関連情報の表示指示が入力された場合、関連情報抽出部21で抽出した表示中のデジタル画像データの関連情報を取得し、表示内容を、デジタル画像データから当該関連情報に切り替える(ステップS211)。この際、ステップS203で立てたフラグを調べ、電子署名の認証結果(改竄あり/なし)も併せて表示する。それから、ステップS212に移行する。

【0079】ステップS212では、入力部23を介して、操作者より画像の表示指示が入力されたか否かを判断し、当該指示が入力された場合は、ステップS207に移行し、表示内容を、関連情報からデジタル画像データにしたがった画像に切り替える。

【0080】以上、本発明の第1実施形態について説明した。

【0081】本実施形態によれば、映像を撮像することで得られたデジタル画像データに、当該データの関連情報が埋め込まれ、さらに、当該関連情報が埋め込まれたデジタル画像データに、当該データの電子署名が付加されて記憶媒体に記憶されるので、当該電子署名を用いて認証を行うことにより、電子署名作成後に当該データに加えられた変更を検出することができ、また、当該データから関連情報を抽出し、その内容を確認することができる。関連情報の埋め込みや電子署名の作成は、映像撮影時に電子カメラ内で行われるので、各種証明や証拠などの撮影に使用した場合、デジタル画像データの改竄などの不正を検出できるとともに証拠としての信頼性を向上させることができる。

【0082】また、本実施形態では、関連情報が埋め込まれたデジタル画像データを圧縮し、電子署名は圧縮画像データに対して作成するようにしている。このようにすることで、記憶媒体に記憶する情報量を減らすことができる。

【0083】なお、本実施形態では、関連情報挿入部13において、受像部11より受け取ったデジタル画像データに関連情報を埋め込んだ後に、圧縮部14により当該データを圧縮しているが、圧縮部14において、受像部11より受け取ったデジタル画像データを圧縮した後、関連情報挿入部13により、当該圧縮画像データに

前記デジタル画像データの関連情報を埋め込むようにしてもよい。この場合、画像再生に際しては、関連情報抽出部21において、関連情報が埋め込まれた圧縮画像データより当該関連情報を抽出した後、伸張部20により伸張するようにすればよい。

【0084】このようにした場合でも、本実施形態と同様、記憶媒体に記憶する情報量を減らすことができる。ただし、このようにすると、関連情報がデジタル画像データの圧縮画像データに対して埋め込まれるため、当該デジタル画像データに与える影響が本実施形態の場合に比べて大きい。

【0085】次に、本発明の第2実施形態について説明する。

【0086】図7は、本発明の第2実施形態が適用された電子カメラの機能構成図である。

【0087】図7に示すように、本実施形態の電子カメラが、図1に示す第1実施形態の電子カメラと異なる点は、関連情報挿入部13に代えて関連情報挿入部13aを用いた点、および、画像データ分割部25と画像データ統合部26を新たに設けた点である。その他については第1実施形態のものと同様である。

【0088】画像データ分割部25は、受像部11より受け取ったデジタル画像データを複数の領域に分割する。たとえば、受け取ったデジタル画像データが1280×960ピクセルである場合、当該データを1280×160ピクセル単位で6つ領域に分割する。そして、分割したデジタル画像データを関連情報挿入部13aへ渡す。

【0089】関連情報挿入部13aは、画像データ分割部25より受け取った分割されたデジタル画像データの関連情報を、関連情報保持部12より取得し、当該情報を、電子透かし技術を利用して、分割されたデジタル画像データの任意の領域に埋め込む。そして、当該デジタル画像データの、関連情報が埋め込まれた領域を含む全ての領域のデータを画像データ統合部26へ渡す。

【0090】画像データ統合部26は、関連情報挿入部13aから渡されたデータを統合しデジタル画像データを復元する。これにより、関連情報が埋め込まれたデジタル画像データを生成し、圧縮部14へ渡す。

【0091】上記の機能構成ブロックは、図3において、これらの機能を実現するためのプログラムをROM64に格納しておき、CPU63により実行させることで実現できる。

【0092】以上、本発明の第2実施形態について説明した。

【0093】本実施形態によれば、関連情報の埋め込みは、複数の領域に分割されたデジタル画像データの任意の領域に対して行われるので、デジタル画像データ全体に対して関連情報を埋め込む場合に比べ、関連情報の埋め込みに使用するメモリのワークエリアやCPUの負荷

を小さくすることができる。すなわち、図3において、RAM 65の容量やCPU 63の処理能力を小さくすることができる。このことは、小型・軽量化が望まれる電子カメラに特に有効である。

【0094】なお、本実施形態では、関連情報の埋め込みを、複数の領域に分割されたデジタル画像データの任意の領域に対して行っているが、任意の領域に関連情報の全てを埋め込むと、当該領域の画質の劣化が危惧される場合は、以下のように修正してもよい。

【0095】すなわち、関連情報挿入部13aにおいて、関連情報を、画像データ分割部25でのデジタル画像データの分割数と同じ数に分割して、各々を、複数の領域に分割された当該デジタル画像データの各領域に対応させる。そして、複数の領域に分割されたデジタル画像データの各領域について、当該領域に、複数の分割された関連情報の対応する部分を埋め込む処理を順次行う。その後、画像データ統合部26により、各々に関連情報の対応する部分が埋め込まれた複数の領域を統合して、関連情報が埋め込まれたデジタル画像データを生成する。

【0096】次に、本発明の第3実施形態について説明する。

【0097】図8は、本発明の第3実施形態が適用された電子カメラの機能構成図である。

【0098】図8に示すように、本実施形態の電子カメラが、図1に示す第1実施形態の電子カメラと異なる点は、関連情報挿入部13および関連情報抽出部21に代えて、電子署名・関連情報挿入部13bおよび電子署名・関連情報抽出部21aを設けた点である。その他については第1実施形態のものと同様である。

【0099】電子署名・関連情報挿入部13bは、電子署名生成部15にて生成された、圧縮部14で生成された圧縮画像データに対する電子署名と、関連情報保持部12に保持された、当該圧縮画像データの元となるデジタル画像データの関連情報とを、電子透かし技術を利用して、当該圧縮画像データに埋め込む。

【0100】電子署名・関連情報抽出部21aは、電子透かし技術を利用して、圧縮画像データに埋め込まれた当該圧縮画像データに対する電子署名と関連情報とを抽出する。

【0101】なお、電子署名・関連情報挿入部13bにおける電子署名および関連情報の埋め込みは、電子署名・関連情報抽出部21aにおいて、当該圧縮画像データからこれらの情報を完全に取り去ることができるように埋め込む必要がある。たとえば、所定の規則にしたがい、圧縮画像データの所定の複数位置に情報を挿入するように、電子署名および関連情報を埋め込む。このようにすることで、電子署名・関連情報抽出部21aにおいて、前記所定の規則にしたがい、圧縮画像データの所定の複数位置から情報を取り去ることで、当該圧縮画像デ

ータから電子署名および関連情報を完全に取り去るように抽出することができる。

【0102】上記の機能構成ブロックは、図3において、これらの機能を実現するためのプログラムをROM 64に格納しておき、CPU 63により実行させることで実現できる。

【0103】次に、本実施形態が適用された電子カメラの動作について説明する。

【0104】まず、本実施形態が適用された電子カメラの撮影時の動作を説明する。

【0105】図9は、図8に示す電子カメラの撮影時の動作を説明するためのフロー図である。

【0106】このフローは、入力部23で受け付けた操作者の指示より、動作モードとして、撮影モードが選択されている場合に実行される。

【0107】まず、受像部11は、レンズで捉えた光学像を電気信号に変換し、さらにデジタル画像データに変換して表示部22に送る（ステップS301）。表示部22は、受け取ったデジタル画像データにしたがった画像を表示する（ステップS302）。

【0108】次に、受像部11は、入力部23を介して、デジタル画像データの記録指示が入力されたか否か、すなわち、シャッターボタンが押されたか否かを判断し（ステップS303）、押された場合にはステップS304へ移行し、押されていない場合はステップS301に戻る。

【0109】ステップS304では、圧縮部14は、受像部11からデジタル画像データを受け取り、これを所定の圧縮方式にしたがって圧縮し、圧縮結果である圧縮画像データを電子署名生成部15に渡す。

【0110】電子署名生成部15は、入力部23を介して操作者より選択された撮影モードが証拠写真モードであるか否かを判断する（ステップS305）。証拠写真モードであると判断した場合は、圧縮部14より受け取った圧縮画像データの電子署名を生成し（ステップS306）、生成した電子署名を圧縮画像データとともに電子署名・関連情報挿入部13bへ渡す。これを受けて、電子署名・関連情報挿入部13bは、この電子署名と関連情報保持部12に保持されている関連情報とを、電子透かし技術を利用して、圧縮画像データに埋め込む（ステップS307）。この際、上述したように、埋め込んだ電子署名および関連情報が圧縮画像データから完全に取り去ることができるように埋め込む。その後、電子署名および関連情報が埋め込まれた圧縮画像データを、記録部17へ渡す。

【0111】一方、ステップS305において、証拠写真モードでないと判断した場合は、圧縮部14より受け取った圧縮画像データを直ちに記録部17へ渡す。

【0112】記録部17は、電子署名生成部15あるいは電子署名・関連情報挿入部13bより受け取った圧縮

画像データを記憶部16に装着されている記憶媒体に記憶する(ステップS308)。この際、電子署名・関連情報挿入部13bより受け取った圧縮画像データを記憶する場合は、証拠写真モードで撮影された旨を示すフラグを当該圧縮画像データに付加して記憶する。

【0113】このようにすることで、撮影モードとして証拠写真モードが選択されている場合、撮影により得たデジタル画像データが圧縮され、この圧縮画像データの電子署名が作成される。そして、デジタル画像データの関連情報と作成した電子署名とが当該圧縮画像データに埋め込まれる。

【0114】次に、本実施形態が適用された電子カメラの画像再生時の動作を説明する。

【0115】図10は、図8に示す電子カメラの画像再生時の動作を説明するためのフロー図である。

【0116】このフローは、入力部23で受け付けた操作者の指示より、動作モードとして、再生モードが選択されている場合に実行される。

【0117】まず、再生部18は、記録部16に装着されている記憶媒体より、圧縮画像データ(図9に示すフローにより記憶媒体に記録されたデータ)を読み出し(ステップS401)、電子署名・関連情報抽出部21aに渡す。なお、圧縮画像データに証拠写真モードで撮影された旨を示すフラグが付加されている場合は、これも読み出して電子署名・関連情報抽出部21aに渡す。

【0118】次に、電子署名・関連情報抽出部21aは、再生部18から受け取った圧縮画像データにフラグが付加されているか否かを調べることで、当該圧縮画像データが証拠写真モードで撮影されたものであるか否かを判断する(ステップS402)。証拠写真モードで撮影されたものである場合、たとえば図5(b)に示すような、証拠写真モードである旨を示すフラグ「1」を図3に示すRAM65等の所定領域に記憶させ、ステップS403に移行する。一方、証拠写真モードで撮影されたものでない場合は、たとえば図5(b)に示すような、通常の写真モードである旨を示すフラグ「0」を図3に示すRAM65等の所定領域に記憶させ、ステップS405に移行する。

【0119】ステップS403において、電子署名・関連情報抽出部21aは、電子透かし技術を利用して、再生部18より受け取った圧縮画像データから電子署名および関連情報を完全に取り去るように抽出する。それから、圧縮画像データを抽出した電子署名とともに電子署名認証部19に渡す。これを受けて、電子署名認証部19は、この電子署名を用いて圧縮画像データの認証を行う(ステップS404)。そして、認証の結果を記憶する。たとえば図5(c)に示すような、圧縮画像データが改竄されたか否かを示すフラグを、図3に示すRAM65の所定領域に記憶させる。

【0120】ステップS405では、伸張部20は、圧

縮画像データを受け取り、これを伸張して、デジタル画像データを得る。表示部22は、このデジタル画像データにしたがった画像を表示する(ステップS406)。

【0121】次に、表示部22は、ステップS402で立てたフラグを調べ、表示中のデジタル画像データが証拠写真モードで撮影されたものであるか否かを判断する(ステップS407)。証拠写真モードで撮影されたものでない場合は、ステップS408に移行し、入力部23を介して、操作者より画像の送り・戻し指示が入力されたか否かを判断する。画像の送り・戻し指示が入力された場合、当該指示により特定される圧縮画像データを記憶部16の記憶媒体から読み出すべく、ステップS401に戻る。一方、画像の送り・戻し指示が入力されていない場合はステップS406に戻る。

【0122】ステップS407において、表示中のデジタル画像データが証拠写真モードで撮影されたものと判断された場合、ステップS409に移行し、入力部23を介して、操作者より関連情報の表示指示が入力されたか否かを判断する。関連情報の表示指示が入力されていない場合はステップS408に移行する。一方、関連情報の表示指示が入力された場合、電子署名・関連情報抽出部21aで抽出した表示中のデジタル画像データの関連情報を取得し、表示内容を、デジタル画像データから当該関連情報に切り替える(ステップS410)。この際、ステップS404で立てたフラグを調べ、電子署名の認証結果(改竄あり/なし)も併せて表示する。それから、ステップS411に移行する。

【0123】ステップS411では、入力部23を介して、操作者より画像の表示指示が入力されたか否かを判断し、当該指示が入力された場合は、ステップS406に移行し、表示内容を、関連情報からデジタル画像データにしたがった画像に切り替える。

【0124】以上、本発明の第3実施形態について説明した。

【0125】本実施形態においても、第1実施形態と同様の効果を得ることができる。

【0126】なお、本発明は上記の各実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【0127】たとえば、上記の各実施形態では、証拠写真モードが選択された場合、関連情報の埋め込み・抽出および電子署名の作成・認証を自動的に行うものについて説明したが、関連情報の埋め込み・抽出および電子署名の作成・認証の各々について、処理を行うか否かを表示部22を介して確認し、当該処理を行う旨の指示が入力部23に入力された場合に、当該処理を行うようにしてもよい。また、関連情報の埋め込みについては、埋め込む情報を特定を表示部22および入力部22を介して、操作者と対話的に行うようにしてもよい。

【0128】また、上記の各実施形態では、電子透かし

技術を利用した関連情報の埋め込み・抽出、および、デジタル画像データに対する電子署名の作成・認証の両方の処理を行うものについて説明したが、いずれか一方の処理のみを行うものでもよい。電子透かし技術を利用した関連情報の埋め込み・抽出を行う電子カメラによれば、デジタル画像データの証拠としての信頼性を向上させることができ、デジタル画像データに対する電子署名の作成・認証を行う電子カメラによれば、デジタル画像データの改竄などの不正を検出することができる。

【0129】また、上記の各実施形態では、画像再生時に、証拠写真モードで撮影されたものについて、電子透かし技術を利用した関連情報の抽出、および、デジタル画像データに対する電子署名の認証を行うものについて説明したが、これらの処理をパーソナルコンピュータなどの情報処理装置に行わせることを前提として、これらの機能を電子カメラから省略するようにしてもよい。

【0130】一例として、上記の第1、2実施形態に示す電子カメラにおいて、証拠写真モードで撮影されたデジタル画像データの検証を行う情報処理装置について説明する。

【0131】図11は、本発明の第1、2実施形態に示す電子カメラにより証拠写真モードで撮影されたデジタル画像データの検証を行う情報処理装置のハードウェア構成図、図12は、図11に示す情報処理装置によりデジタル画像データの検証を行う際の動作を説明するためのフロー図である。

【0132】まず、CPU73の指示により、コネクタ79を介して接続されたフラッシュメモリ79あるいはI/Oポート783を介して接続された図3に示す電子カメラから圧縮画像データが読み込まれ、RAM75に格納される(ステップS401)。なお、ROM74には、各種プログラムが格納されており、CPU73により実行することで、図11に示す各部を統括的に制御する。また、図1、図7に示す再生部18、電子署名認証部19、伸張部20、および、関連情報抽出部21をプロセスとして実現する。ROM74は、たとえばCD-ROMなどの可搬性を有する記憶媒体により構成されたものでもよい。

【0133】次に、CPU73は、ROM74から電子署名を認証するための検証鍵(当該電子署名を作成する際に用いた秘密鍵(署名鍵)と対の公開鍵)を取り出し、RAM75に格納された圧縮画像データに付加されている電子署名を検証し、その結果をRAM75に格納する(ステップS502)。

【0134】次に、CPU73は、圧縮画像データを伸長してデジタル画像データを復元し、これをRAM75に格納する(ステップS503)。それから、電子透かし技術を利用して、復元したデジタル画像データに埋め込まれた当該データの関連情報を抽出し、RAM75に格納する(ステップS504)。

【0135】次に、CPU73は、キー入力装置72に入力された操作者の指示にしたがい、復元したデジタル画像データにしたがった画像、抽出した関連情報、および、電子署名の検証結果のいずれか1つあるいはこれ等の組合せを、表示装置72に表示させる(ステップS505)。

【0136】このようにすることで、上記の第1、2実施形態に示す電子カメラにおいて、証拠写真モードで撮影されたデジタル画像データの検証を情報処理装置に行うことが可能となる。

【0137】

【発明の効果】以上説明したように、本発明によれば、生成したデジタル画像データの改竄防止や証拠としての信頼性向上に好適な記録装置を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態が適用された電子カメラの機能構成図である。

【図2】図1に示す圧縮部14での圧縮にJPEG方式を用いた場合において、記憶部16に装着された記憶媒体に記録されるデータの構成を示した図である。

【図3】図1に示す電子カメラのハードウェア構成の一例を示す図である。

【図4】図1に示す電子カメラの撮影時の動作を説明するためのフロー図である。

【図5】図3に示すRAM65に記憶される各種フラグを説明するための図である。

【図6】図1に示す電子カメラの画像再生時の動作を説明するためのフロー図である。

【図7】本発明の第2実施形態が適用された電子カメラの機能構成図である。

【図8】本発明の第3実施形態が適用された電子カメラの機能構成図である。

【図9】図8に示す電子カメラの撮影時の動作を説明するためのフロー図である。

【図10】図8に示す電子カメラの画像再生時の動作を説明するためのフロー図である。

【図11】本発明の第1、2実施形態に示す電子カメラにより証拠写真モードで撮影されたデジタル画像データの検証を行う情報処理装置のハードウェア構成図である。

【図12】図11に示す情報処理装置によりデジタル画像データの検証を行う際の動作を説明するためのフロー図である。

【符号の説明】

11：受像部、12：関連情報保持部、13、13a：関連情報挿入部

13b：電子署名・関連情報挿入部、14：圧縮部、15：電子署名生成部

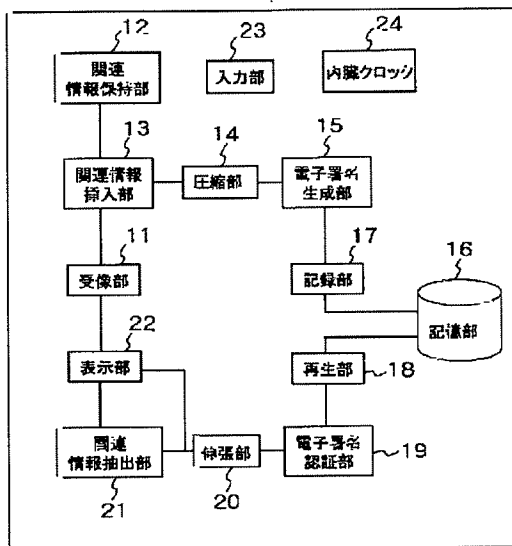
16：記憶部、17：記録部、18：再生部、19：電子署名認証部、20：伸張部

21：関連情報抽出部、21a：電子署名・関連情報抽出部、22：表示部
 23：入力部、24：内蔵クロック、25：画像データ分割部
 26：画像データ統合部、51：CCD、52：バッファ、53：A/D変換器
 54：タイミング発生器、55：駆動回路、56：DRAM、57：圧縮・伸張回路

58：フラッシュメモリ、59,79：コネクタ、60：ビデオ信号発生器
 61：D/A変換器、62：液晶ディスプレイ、63,73：CPU
 64,74：ROM、65,75：RAM、66,76：キー入力装置
 67：クロック、68,78：I/Oポート、72：表示装置

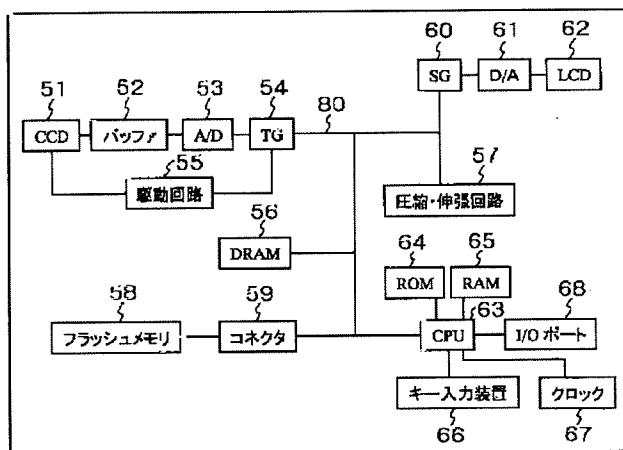
【図1】

図1



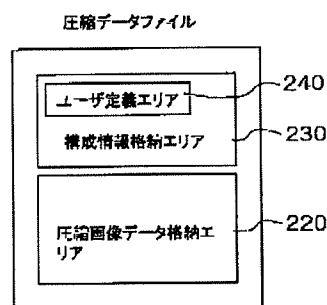
【図3】

図3



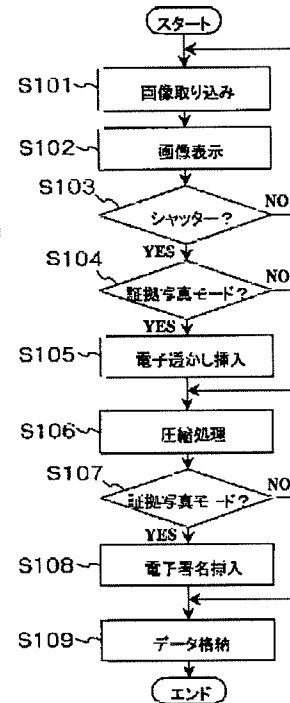
【図2】

図2



【図4】

図4

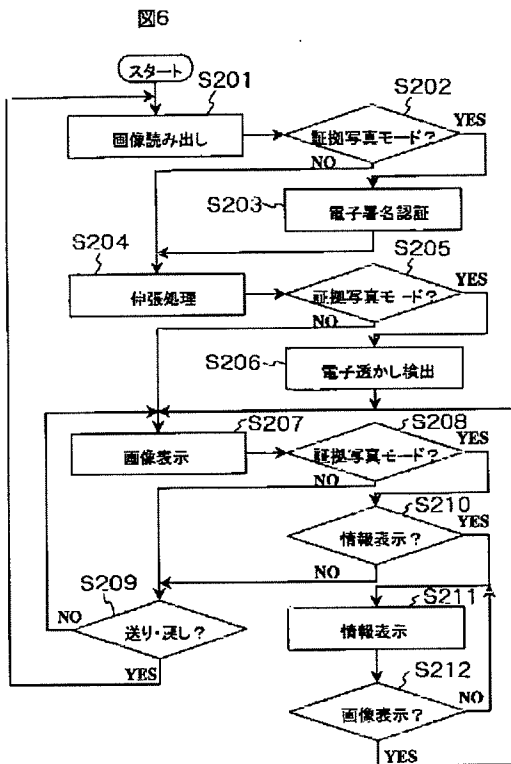


【図5】

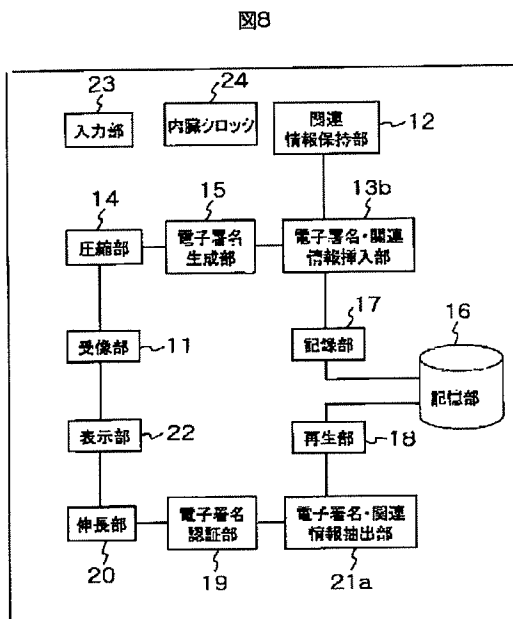
図5

- (a) 撮影モード 0/1
 0: 通常モード
 1: 証拠写真モード
- (b) 再生モード 0/1
 0: 通常モード
 1: 証拠写真モード
- (c) 改ざん検知フラグ 0/1
 0: 改ざんなし
 1: 改ざんあり

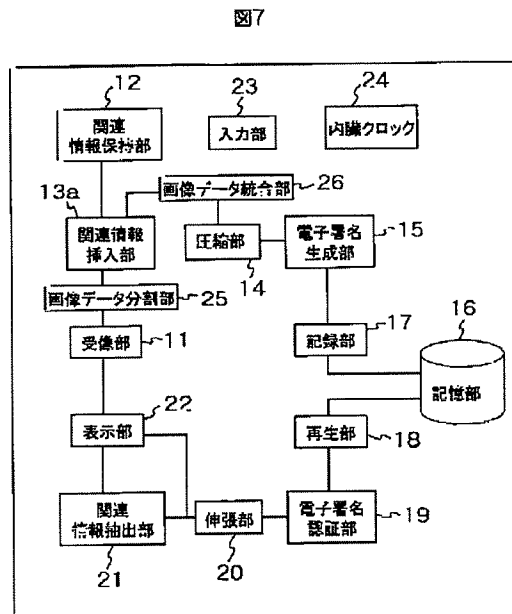
【図6】



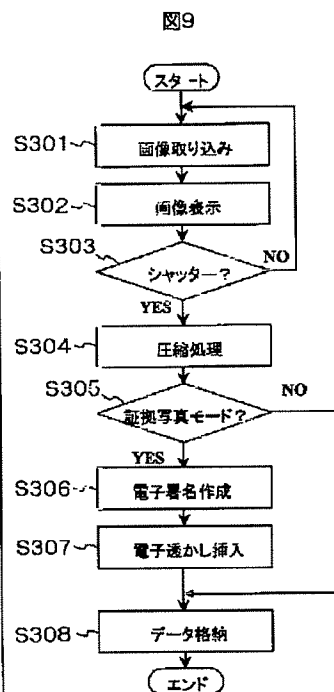
【图8】



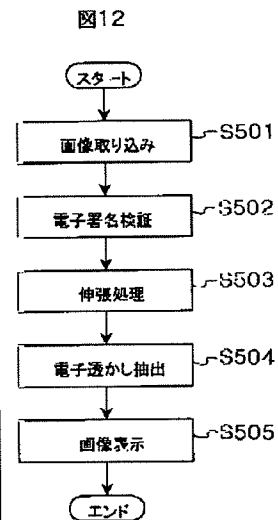
【図7】



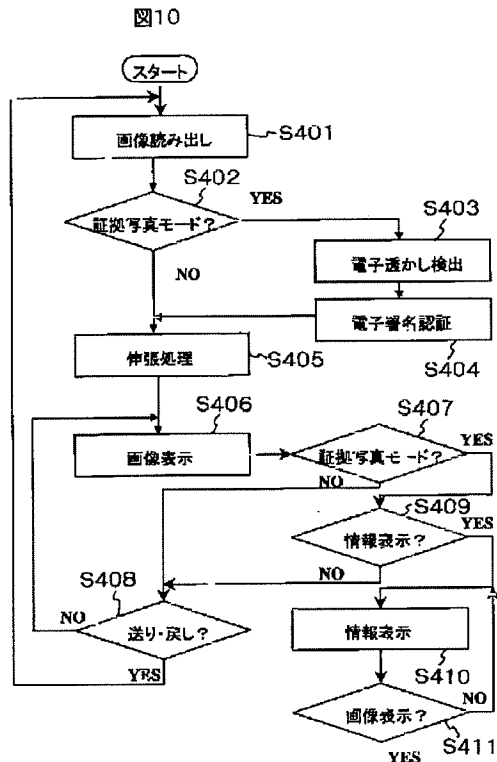
【図9】



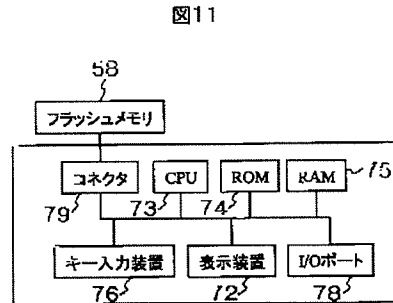
【图 12】



【図10】



【図11】



フロントページの続き

(51)Int.Cl.⁷
// H04N 101:00

識別記号

F I
B 4 1 J 29/00

(参考)

Z

(72)発明者 吉浦 裕
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 金野 千里
東京都品川区南大井六丁目27番18号 株式会社日立製作所情報コンピュータグループ内

(72)発明者 黒須 豊
神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内

Fターム(参考) 2C061 CL10
2C087 AA13 BA03 BB10 BC07 BD05
BD40 DA13
5B057 AA11 CA12 CA16 CB12 CB16
CE08 CE09 DA06
5C022 AA13 AC03 AC11 AC32 AC42
AC52 AC54 AC69 AC75 AC80
5C076 AA14 AA16 AA19 AA36 BA06